

Patent number: JP2001229614
Publication date: 2001-08-24
Inventor: KAWAMAE OSAMU; NOGUCHI TAKAHARU; TAKEUCHI TOSHIFUMI
Applicant: HITACHI LTD
Classification:
- **international:** G11B20/10; G06F12/14; G06T1/00; G09C5/00; H04N1/387; H04N5/91; H04N5/92
- **european:**
Application number: JP20000058962 20000303
Priority number(s): JP20000058962 20000303; JP19990349162 19991208

[illegible]

BEST AVAILABLE COPY

(19)日本国特許庁(JP)

(12)公開特許公報 (A)

(11)特許出願公開番号

特開2001-229614

(P2001-229614A)

(43)公開日 平成13年8月24日(2001.8.24)

(51)Int. Cl. ⁷	識別記号	F I	テ-マ-ド(参考)
G 1 1 B 20/10	3 0 1	G 1 1 B 20/10	H 5B017
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 0 1 A 5B057
G 0 6 T 1/00	5 0 0	G 0 6 T 1/00	3 2 0 E 5C053
G 0 9 C 5/00		G 0 9 C 5/00	5 0 0 B 5C076
			5D044
審査請求 未請求 請求項の数 2 0 O L		(全 2 6 頁) 最終頁に続く	

(21)出願番号 特願2000-58962(P2000-58962)

(22)出願日 平成12年3月3日(2000.3.3)

(31)優先権主張番号 特願平11-349162

(32)優先日 平成11年12月8日(1999.12.8)

(33)優先権主張国 日本(JP)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 川前 治

神奈川県横浜市戸塚区吉田町292番地 株

式会社日立製作所デジタルメディア開発本
部内

(72)発明者 竹内 敏文

神奈川県横浜市戸塚区吉田町292番地 株

式会社日立製作所デジタルメディア開発本
部内

(74)代理人 100078134

弁理士 武 頭次郎

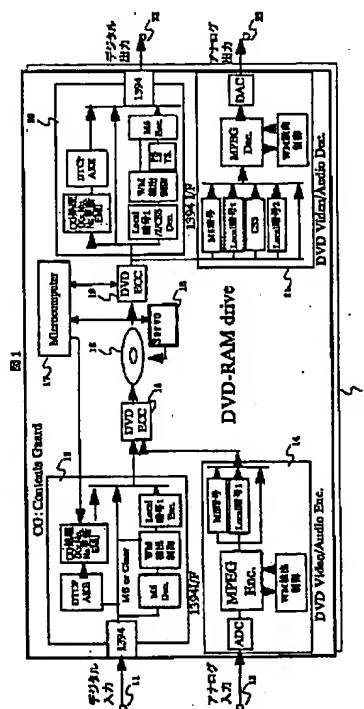
最終頁に続く

(54)【発明の名称】データ記録装置およびデータ再生装置およびデータ記録方法およびデータ再生方法

(57)【要約】

【課題】 著作権のあるデータが不正に記録あるいは再生されることを防止すること。

【解決手段】 デジタル入出力及びアナログ入出力を備えたビットストリーム記録再生装置、またはRTRW記録再生装置において、適切なWM検出制御手段と暗号のエンコード/デコードを備える。



【特許請求の範囲】

【請求項1】 デジタルデータを入力する入力端子と、転送されたデジタルデータを受信するインターフェイス手段と、前記転送されたデジタルデータを記録媒体に記録するための記録処理を行う記録処理手段と、データを記録媒体に記録する記録手段とを、備えたデータ記録装置において、

前記インターフェイス手段は、

前記デジタルデータが暗号化されている場合には、暗号を復号する復号手段と、

復号されたデジタルデータから電子透かし情報を検出する第1の検出手段と、

前記デジタルデータを暗号化する第1の暗号手段とを、備えたことを特徴とするデータ記録装置。

【請求項2】 請求項1において、

アナログ信号を入力する入力端子と、アナログ信号をデジタル信号に変換するAD変換手段と、変換された前記デジタル信号を圧縮する圧縮手段とを備え、

前記圧縮手段は、

電子透かし情報を検出する第2の検出手段と、

圧縮されたデータを暗号化する第2の暗号手段とを、備えたことを特徴とするデータ記録装置。

【請求項3】 アナログ信号を入力する入力端子と、アナログ信号をデジタル信号に変換するAD変換手段と、変換された前記デジタル信号を圧縮する圧縮手段と、圧縮されたデジタル信号を記録媒体に記録するための記録処理を行う記録処理手段と、データを記録媒体に記録する記録手段とを、備えたデータ記録装置において、

前記圧縮手段は、

電子透かし情報を検出する第2の検出手段と、

圧縮されたデータを暗号化する第2の暗号手段とを、備えたことを特徴とするデータ記録装置。

【請求項4】 請求項3において、

デジタルデータを入力する入力端子と、転送されたデジタルデータを受信するインターフェイス手段とを備え、

前記インターフェイス手段は、

前記デジタルデータが暗号化されている場合には、暗号を復号する復号手段と、

復号されたデジタルデータから電子透かし情報を検出する第1の検出手段と、

前記デジタルデータを暗号化する第1の暗号手段とを、備えたことを特徴とするデータ記録装置。

【請求項5】 請求項4において、

前記第1の暗号手段と前記第2の暗号手段で同じ暗号化を行う場合には、前記第1の暗号手段と前記第2の暗号手段とを共通化することを特徴とするデータ記録装置。

【請求項6】 データを記録媒体から再生する再生手段と、記録媒体から読み出したデータの再生処理を行う再

生処理手段と、再生処理後のデジタルデータを送信するインターフェイス手段と、デジタルデータを出力する出力端子とを、備えたデータ再生装置において、前記インターフェイス手段は、

前記再生処理後のデジタルデータが暗号化されている場合には、暗号を復号する第1の復号手段と、

復号されたデジタルデータから電子透かし情報を検出する第1の検出手段と、

前記デジタルデータを暗号化する第1の暗号手段と

10 を、備えたことを特徴とするデータ再生装置。

【請求項7】 請求項6において、

再生処理されたデータを伸長する伸長手段と、デジタル信号をアナログ信号に変換するDA変換手段と、アナログ信号を出力する出力端子とを備え、

再生処理され伸長処理される前のデジタルデータが暗号化されている場合には、暗号を復号する第2の復号手段を備え、

前記伸長手段は、電子透かし情報を検出する第2の検出手段を、備えたことを特徴とするデータ再生装置。

20 【請求項8】 データを記録媒体から再生する再生手段と、記録媒体から読み出したデータの再生処理を行う再生処理手段と、再生処理されたデータを伸長する伸長手段と、デジタル信号をアナログ信号に変換するDA変換手段と、アナログ信号を出力する出力端子とを、備えたデータ再生装置において、

再生処理後のデジタルデータが暗号化されている場合には、暗号を復号する第2の復号手段を備え、

前記伸長手段は、電子透かし情報を検出する第2の検出手段を、備えたことを特徴とするデータ再生装置。

30 【請求項9】 請求項8において、

再生処理後のデジタルデータを送信するインターフェイス手段と、デジタルデータを出力する出力端子とを備え、

前記インターフェイス手段は、

このインターフェイス手段に入力される再生処理後のデジタルデータが暗号化されている場合には、暗号を復号する第1の復号手段と、

復号されたデジタルデータから電子透かし情報を検出する第1の検出手段と、

40 前記デジタルデータを暗号化する第1の暗号手段とを、備えたことを特徴とするデータ再生装置。

【請求項10】 請求項7または9において、

前記第1の復号手段と前記第2の復号手段で同じ復号化を行う場合には、前記第1の復号手段と前記第2の復号手段を共通化することを特徴とするデータ再生装置。

【請求項11】 データを入力し、前記データを記録するデータ記録方法において、

前記入カデータに暗号がかけられている場合には、一旦暗号を復号して、前記入カデータに含まれている付加情報を検出し、

この検出結果に従って、前記入カデータの記録を制御し、再び、所定の方法で入力データを暗号化して、記録データとするようにしたことを特徴とするデータ記録方法。

【請求項12】 請求項11において、前記入カデータの復号は、前記付加情報を検出できるデータフォーマットまで復号するようにしたことを特徴とするデータ記録方法。

【請求項13】 請求項11において、前記入カデータに暗号がかけられていない場合は、前記入カデータに含まれている付加情報を検出し、この検出結果に従って、前記入カデータの記録の制御を行い、必要に応じて、再び、所定の方法で入力データを暗号化して、記録データとするようにしたことを特徴とするデータ記録方法。

【請求項14】 請求項11において、前記入カデータは転送するためのデータ列フォーマットで構成されており、記録データは異なるデータ列フォーマットで記録するときには、前記復号を行って、再度暗号化を行うまでの間に、データ列フォーマットの変換を行うようにしたことを特徴とするデータ記録方法。

【請求項15】 記録媒体からデータを再生し、再生データを出力するデータ再生方法において、前記再生データに暗号がかけられている場合には、一旦暗号を復号して、前記再生データに含まれている付加情報を検出し、この検出結果に従って、前記再生データの出力を制御し、再び、所定の方法で再生データを暗号化して、出力データとするようにしたことを特徴とするデータ再生方法。

【請求項16】 請求項15記載において、前記再生データの復号は、前記付加情報を検出できるデータフォーマットまで復号するようにしたことを特徴とするデータ再生方法。

【請求項17】 請求項15記載において、前記再生データに暗号がかけられていない場合は、前記再生データに含まれている付加情報を検出し、この検出結果に従って、前記再生データの出力の制御を行い、必要に応じて、再び、所定の方法で再生データを暗号化して、出力データとするようにしたことを特徴とするデータ再生方法。

【請求項18】 請求項15記載において、前記入カデータは記録媒体に記録するためのデータ列フォーマットで構成されており、出力データは異なるデータ列フォーマットで出力するときには、前記復号を行って、再度暗号化を行うまでの間に、データ列フォーマットの変換を行うようにしたことを特徴とするデータ再生方法。

【請求項19】 請求項4において、前記第1の検出手段と前記第2の検出手段を兼用したこ

とを特徴とするデータ記録装置。

【請求項20】 請求項9において、前記第1の検出手段と前記第2の検出手段を兼用したことを特徴とするデータ再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、画像や音声データを記録および/または再生する装置並びに方法に係り、特に、記録媒体の複写管理情報に応じて記録再生あるいは再生あるいは記録の動作を制御するようにした技術に関する。

【0002】

【従来の技術】DVD-ROMは、CD-Rの約7倍の容量を持つ媒体である。これにはPC用のプログラムコードだけでなく、映像や音声データを圧縮することで映画ソフトを記録することもできる。DVDにデータを記録する記録媒体としては、DVD-RAMや、DVD-R、DVD-RWがある。これらにも大容量のデータを記録することが出来るため、映画などのソフトウェアがそのままデジタル複写されることを防止しなければならない。このため、不正複写防止技術が重要になる。

【0003】この技術の一つとして、電子透かし技術があり、その標準化について日経BP社「日経エレクトロニクス」(1998.5.18 P31~P32)に記載されている。

【0004】また、電子透かし技術とは別に、IEEE1394を使って機器間でのデータのやり取りにおける不正複写防止技術についても、日経BP社「日経エレクトロニクス」(1998.3.23 P47~P53)に記載されている。

【0005】

【発明が解決しようとする課題】しかし、DVD-RAMドライブのように、デジタル/アナログ入出力を備えた機器については、これらの技術だけで不正複写を防止することは困難であり、また容易に回避されてしまうこともある。また、PC内部では、さらに複雑なデータのやり取りが行われるため、複写制御の抜け道も発生しやすくなる。

【0006】このため、電子透かし技術やIEEE1394複写防止技術も含めて、複数の複写制御技術を適切に組み合わせて用いるシステムを構築することが求められている。

【0007】本発明は上記の点に鑑みなされたもので、その目的とするところは、デジタル/アナログ入出力を備えたビットストリーム記録再生装置あるいはRTRW記録再生装置において、著作権のあるデータが不正に記録または再生されることを防止することにある。

【0008】

【課題を解決するための手段】上記目的を達成するために、本発明は、例えば、デジタルデータを入力する入力端子と、転送されたデジタルデータを受信するイン

ターフェイス手段と、アナログ信号を入力する入力端子と、アナログ信号をデジタル信号に変換するAD変換手段と、この変換されたデジタル信号を圧縮する圧縮手段と、前記転送されたデジタルデータと圧縮されたデジタル信号を記録媒体に記録するための記録処理を行う記録処理手段と、データを記録媒体に記録する記録手段とを、備えたデータ記録装置において、前記インターフェイス手段は、前記デジタルデータが暗号化されている場合には、暗号を復号する復号手段と、復号されたデジタルデータから電子透かし情報を検出する第1の検出手段と、前記デジタルデータを暗号化する第1の暗号手段とを備え、前記圧縮手段は、電子透かし情報を検出する第2の検出手段と、圧縮されたデータを暗号化する第2の暗号手段とを備える。

【0009】また、本発明は、例えば、データを記録媒体から再生する再生手段と、記録媒体から読み出したデータの再生処理を行う再生処理手段と、再生処理後のデジタルデータを送信するインターフェイス手段と、デジタルデータを出力する出力端子と、再生処理されたデータを伸長する伸長手段と、デジタル信号をアナログ信号に変換するDA変換手段と、アナログ信号を出力する出力端子とを、備えたデータ再生装置において、前記インターフェイス手段は、このインターフェイス手段に入力される再生処理後のデジタルデータが暗号化されている場合には、暗号を復号する第1の復号手段と、復号されたデジタルデータから電子透かし情報を検出する第1の検出手段と、前記デジタルデータを暗号化する第1の暗号手段とを備え、また、再生処理され伸長処理される前のデジタルデータが暗号化されている場合には、暗号を復号する第2の復号手段を備え、前記伸長手段は、電子透かし情報を検出する第2の検出手段を備える。

【0010】

【発明の実施の形態】以下、本発明の実施の形態を、図面を用いて説明する。

【0011】図1は、本発明の1実施形態に係る、複写制御情報を含むデータを記録再生する記録再生装置の構成を示すブロック図である。本実施形態は、例えば、DVD-RAMドライブのような記録再生を行う機器への適用例について示すが、本発明は、記録再生装置に限定されるものではなく、記録装置や再生装置にも適用されるものであって、本実施形態（および後述の実施形態）の記録再生装置には、記録装置や再生装置がその一部として含まれているものとして理解されたい。

【0012】また、データ転送のインターフェース（以下、I/Fと記す）として、以下の説明では、IEEE1394を例にとるが、I/Fとしてはこれ以外にも、ATAPIやSCSI、USBなどが考えられ、I/Fの種別は特に限定されるものではない。また、本実施形態（および後述の実施形態）は、例えば、DVD-R

AMのような記録再生可能な媒体に記録再生を行う装置について示すが、記録媒体は光ディスクに限定されるものではなく、データを記録再生または再生する記録媒体全般にあてはまる。

【0013】図1において、10はビットストリーム（Bit-stream）記録再生可能なDVD-RAMドライブ、11はデジタル入力端子、12はIEEE1394 I/F、13はアナログ入力端子、14はDVDビデオ/オーディオエンコーダ、15はDVD誤り訂正符号付加手段、16はDVDディスク、17はマイクロコンピュータ、18はサーボ手段、19はDVD誤り訂正手段、20はIEEE1394 I/F、21はDVDビデオ/オーディオデコーダ、22はデジタル出力端子、23はアナログ出力端子である。

【0014】次に、本実施形態の動作を説明する。

【0015】ここではまず、動画や音声データを例えばMPEG（Moving Picture Experts Group）などの方式で圧縮し、ビットストリームデータ列で記録するDVD-RAMドライブの動作について説明する。DVD-RAMドライブ1.0への信号入力としては、デジタル信号で入力される場合と、アナログ信号で入力される場合とがある。そのため、DVD-RAMドライブ1.0は、どちらの信号に対しても処理が可能なように処理手段を備える必要がある。それぞれの入力に対する動作を、図1とともに図2、3を用いて説明する。

【0016】図2は、図1におけるIEEE1394 I/F 12の構成を示したものである。同図において、31はIEEE1394信号受信手段、32はDTC（Digital Transmission Content Protection）で採用された方式に則って複写制御を行うDTC手段、33はCG（Contents Guard）方式に則って複写制御を行うCG処理手段、34はM6暗号のデコード手段、35はウォーターマーク（電子透かし；以下、WMと記す）を検出し、それによって制御するWM検出制御手段、36は所定の暗号化を行う暗号1エンコーダである。

【0017】IEEE1394 I/Fを介してデジタル入力で受け取った信号は、IEEE1394信号受信手段31で受信され、転送データがとり出される。DTC手段32は、機器間認証、コピー制御伝送、コンテンツ暗号化により、IEEE1394バス上を伝送するコンテンツを保護するものであり、データ転送を行う機器間での相互の認証と暗号を解くための鍵情報の受け渡しを行い、CG処理手段33は、受信した鍵情報を更新し、新たな鍵情報を記録情報として記録する。

【0018】ここで、転送データに著作権のような権利があるものは、暗号をかけることによりデータを転送途中で読み出すことができないようにしてある。IEEE1394ではM6暗号が採用されている。権利の無いものについては、暗号化されずクリアな信号として転送される。

【0019】そのため、M6暗号がかかったデータはデコード手段34によってM6暗号をデコードして、WM検出可能なデータとし、WM検出制御手段35によりWMを検出し、検出結果にしたがって、出力を制御する。WM検出の結果、不正にコピーしたデータでなく、記録媒体への記録が許可されているデータであるならば、暗号1エンコーダ36により、所定の暗号化を行い、DVD誤り訂正符号付加手段15へ送る。ここで、暗号1はM6暗号と同じ暗号を用いても構わない。同じ暗号を用いることで、暗号の復号回路も共通化が図れるため、回路を簡略することができる。

【0020】また、暗号がかかっていないデータについても、不正にコピーされた可能性があるため、WM検出を行うようにする。WMが検出された場合には、WMにしたがって制御され、必要に応じて、暗号1エンコーダ36により、所定の暗号化を行い、DVD誤り訂正符号付加手段15へ送る。

【0021】WM検出ではDVDディスクに記録するために、コピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。

【0022】WM検出制御手段35は、IEEE1394信号受信手段31からの転送データに対してWM検出を行うものである。このWM検出が転送されたデータからそのまま検出が可能であれば、その状態から検出を行うが、例えば転送データがMPEG圧縮によるビットストリームであるのに対して、ベースバンドの状態からの検出に対応したWM検出であれば、一旦ビットストリームからベースバンドに変換してWMを検出し、その後、元の状態に逆変換して戻すようにする。ここで、変換するレベルは、完全にベースバンドまで変換しなくても、WM検出が可能な段階まで変換を行えば良い。この時に用いるMPEGエンコーダ・デコーダは、DVDビデオ/オーディオエンコーダ14、DVDビデオ/オーディオデコーダ21と兼用することも可能である。

【0023】ここでは、MPEG圧縮変換について述べたが、WM検出するために必要があれば、WMの検出方式に併せた変換もしくは変換の一部を行い、WM検出後もとの状態に逆変換することにより、最適にWM検出を行うことが可能となる。また、この変換はWMの書き換えや追加が必要な場合にも適応させることが出来る。

【0024】図3は、図1におけるDVDビデオ/オーディオエンコーダ14の構成を示したものである。同図において、41はADコンバータ、42はMPEGエンコーダ、43はWM検出制御手段、44はM6暗号エンコーダ、45は暗号2エンコーダである。

【0025】映像信号や音声信号などのアナログ信号は、ADコンバータ41によりデジタル化される。ここでは図示していないが、映像信号の場合には、通常、マクロビジョン信号と呼ばれるコピー防止信号が付加されており、この信号が検出された場合には、コピーを禁

止するように制御する。

【0026】次に、デジタル化されたデータはMPEGのような圧縮方式で圧縮される。同時にWM検出制御43により、WMを検出し、WMが検出された場合にはWMにしたがって制御される。WMが検出されなかったり、データに権利が無いことを示すWMであった場合には、記録するデータを暗号化する必要はないので、MPEGエンコードの後、そのままDVD誤り訂正符号付加手段15へ送る。

10 【0027】WM検出の結果、不正にコピーしたデータでなく、記録媒体への記録が許可されているデータであるならば、M6暗号エンコーダ44または暗号2エンコーダ45により、所定の暗号化を行い、DVD誤り訂正符号付加手段15へ送る。

【0028】WM検出ではDVDディスクに記録するために、コピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。ここで、暗号2はM6暗号またはM1暗号と同じ暗号を用いても構わない。同じ暗号を用いることで、暗号の復号回路も共通化が図れるため、回路を簡略することができる。

20 【0029】このように、図2、3で示したIEEE1394I/F12、および、DVDビデオ/オーディオエンコーダ14からの出力を受け取り、図1のDVD誤り訂正符号付加手段15において、誤り訂正のための符号を付加するとともに、DVDディスク16に記録できるフォーマットに変換する。マイクロコンピュータ17は、記録再生のためのシステム制御を行い、サーボ手段18をコントロールして、DVDディスクの回転やアクセスを制御する。また、図2で示したCG処理における鍵情報のやり取りも行う。

30 【0030】再生時も、記録時と同様デジタル出力系とアナログ出力系があり、それぞれの出力に対する動作を、図1とともに図4、5、6を用いて説明する。

【0031】図4は、図1におけるIEEE1394I/F20の構成を示したものである。同図において、41はCG (Contents Guard) 方式に則って複写制御を行うCG処理手段、42はDTCFで採用された方式に則って複写制御を行うDTCF手段、43はM6暗号のデコード手段、44はCSS (Contents Scramble System) のデコード手段、45は暗号1のデコード手段、46は暗号2のデコード手段、47はWMを検出し、それに従って制御するWM検出制御手段、48はプログラムストリームをトランスポートストリームに変換するPS→TS変換手段、49はM6暗号エンコーダ、50はIEEE1394信号受信手段である。

【0032】DVDディスクから再生されたデータは、DVD誤り訂正手段19で復調及び誤り訂正され、デジタル出力系とアナログ出力系へ送られる。

【0033】CG処理手段41は、データ中に含まれた鍵情報を更新し、新たな鍵情報を記録情報としてDTC

P手段42へ送る。DTC P手段42は、データ転送を行う機器間での相互の認証と暗号を解くための鍵情報の受け渡しを行う。ここで、転送データに著作権のような権利があるものは、暗号をかけることによりデータを転送途中で取り出しても正しく読むことができないようにして転送する。権利の無いものについては、暗号化せずクリアな信号として転送する。

【0034】誤り訂正後のデータは暗号がかかっている場合には、暗号化された方式に従ってデコードを行う。DVD-ROMディスクのデータには、CSSの暗号がかけられており、これに対応したデコーダ（デコード手段44）が必要である。記録時には、デジタル入力系とアナログ入力系で、M6暗号と暗号1、暗号2の3種の暗号があったため、これらの対応した3種のデコーダ（デコード手段43、45、46）を記したが、仮にこれらが同じ暗号を用いて記録されている場合には、それに対応してデコーダは兼用できる。各デコーダによりWM検出可能なデータまでデコードし、WM検出制御47によりWMを検出し、検出結果にしたがって、出力を制御する。

【0035】WM検出の結果、不正に記録されたデータでなく、データの転送が許可されているデータであるならば、M6暗号エンコーダ49により暗号化を行い、IEEE1394信号受信手段50へ送る。

【0036】また、暗号がかかっていないデータについても、不正にコピーされた可能性があるため、WM検出を行うようにする。ここでWMが検出された場合には、WMにしたがって制御され、必要に応じてM6暗号化を行い、IEEE1394信号受信手段50へ送る。

【0037】WM検出ではコピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。仮に、記録時にWMの更新が既に行われていて、再生時に必要が無ければ更新は行わない。

【0038】なお、ここでは、PS→TS変換手段48はWM検出制御手段47の後段で処理する例として示したが、PS→TS変換手段48の処理の後にWM検出制御を行うようにしても構わない。すなわち、PS→TS変換処理とWM検出制御の順番は入れ替えることが可能である。例えば、図14は図4の信号の流れの一部を入れ替えたものである。

【0039】ここで、WM検出制御手段47は、記録媒体からの再生データに対してWM検出を行うものである。このWM検出が再生されたデータからそのまま検出が可能であれば、その状態から検出を行うが、例えばWM検出がトランスポートストリームや、プログラムストリームの状態のどちらかに対応したものであれば、ストリーム変換の適切な部分でWM検出を行うようにする。また、それらのストリームの中間レベルでWM検出が可能ならば、適切なレベルの信号を用いてWM検出を行うようにする。もちろん、一旦ストリームの変換を行い、

WMを検出した後に再び元のトリームに変換しても構わない。また、図4にも示したように、PS→TS変換が必要ない場合には、変換を行わずにWM検出し、出力することも可能である。

【0040】また、再生データがMPEG圧縮によるビットストリームであるのに対して、ベースバンドの状態からの検出に対応したWM検出であれば、一旦ビットストリームからベースバンドに変換してWMを検出し、その後、元の状態に逆変換して戻すようにする。ここで、変換するレベルは、完全にベースバンドまで変換しなくても、WM検出が可能な段階まで変換を行えば良い。

【0041】このように、WM検出が可能なレベルまでデータ状態を変換するための構成とすることにより、余分な回路の増加を防止することが出来る。ここでは、MPEG圧縮と転送ストリーム変換について述べたが、WM検出するために必要があれば、WMの検出方式に併せた変換もしくは変換の一部を行い、WM検出後にもとの状態に逆変換することにより、最適にWM検出を行うことが可能となる。また、この変換はWMの書き換えや追加が必要な場合にも適応させることが出来る。

【0042】ここで、転送するデータは、トランスポートストリーム（TS）とプログラムストリーム（PS）の2種類あり、データ転送に応じて、変換する必要がある。MPEG-2システムの2種のストリームの構成の違いを、図5に示す。トランスポートストリームは、188バイトの固定長パケットを単位として、誤りの発生し易いATM通信やデジタル放送などに用いられる。プログラムストリームは、複数の可変長のPESパケットから構成される複数のパックからなり、CD-ROMや磁気テープなどの誤りが発生しにくいメディアに用いられる。

【0043】このようにストリームの構成の違いがあるため、DVDディスクから再生されたストリームはPSであるが、転送するメディアによっては、PS→TS変換する必要がある。そのため、図4において、プログラムストリームをトランスポートストリームに変換するPS→TS変換手段48により、ストリームを変換してからM6暗号化を行い、IEEE1394信号受信手段50へ送る。

【0044】M6暗号をエンコードしたデータは、IEEE1394信号受信手段50を介してデジタル出力端子23から転送データとして出力される。

【0045】図6は、図1におけるDVDビデオ/オーディオデコーダ21の構成を示したものである。同図において、51はM6暗号のデコード手段、52はCSSのデコード手段、53は暗号1のデコード手段、54は暗号2のデコード手段、55はMPEGデコーダ、56はWM検出制御手段、57はDAコンバータである。

【0046】DVDディスク16から再生されたデータは、DVD誤り訂正手段19で復調及び誤り訂正され、

ディジタル出力系とアナログ出力系へ送られる。

【0047】誤り訂正後のデータは暗号がかかっている場合には、暗号化された方式に従ってデコードを行う。DVD-ROMディスクのデータには、CSSの暗号がかかけられており、これに対応したデコーダ（デコード手段52）が必要である。記録時には、ディジタル入力系とアナログ入力系で、M6暗号と暗号1、暗号2の3種の暗号があったため、これらの対応した3種のデコーダ（デコード手段51、53、54）を記したが、仮にこれらが同じ暗号を用いて記録されている場合には、それに対応してデコーダは兼用できる。各デコーダにより復号され、MPEGデコーダ55により映像信号と音声信号にデコードされる。

【0048】ここで、WM検出制御手段56によりWMを検出し、検出結果にしたがって、出力を制御する。WM検出の結果、不正に記録されたデータでなく、データの出力が許可されているデータであるならば、DAコンバータ57を介してアナログ出力端子23から出力する。また、暗号がかかっていないデータについても、不正にコピーされた可能性があるため、WM検出を行うようにする。ここでWMが検出された場合にはWMにしたがって制御される。

【0049】WM検出ではコピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。仮に、記録時にWMの更新が既に行われていて、再生時に必要が無ければ更新は行わない。

【0050】ここでは図示していないが、映像信号の場合には通常、マクロビジョン信号と呼ばれるコピー防止信号が付加されるため、DAコンバータ57によりディジタル化されたアナログ出力にも、同様にマクロビジョン信号を付加して、コピーを禁止するように制御する。

【0051】ここで、図2、3、4、6の説明において、説明をわかりやすくするためWM検出制御手段を独立に示したが、記録系側においてWM検出制御手段35とWM検出制御手段43とを兼用することも可能であり、また、再生系側においてWM検出制御手段47とWM検出制御手段56とを兼用することも可能である。

【0052】図7は、本発明の他の実施形態に係る、複写制御情報を含むデータを記録再生する記録再生装置の構成を示すブロック図である。

【0053】同図において、70はRTRW (Real Time Read Write) フォーマットで記録再生可能なDVD-RAMドライブ、71はディジタル入力端子、72はIEEE1394I/F、73はアナログ入力端子、74はDVDビデオ/オーディオエンコーダ、75はDVD誤り訂正符号付加手段、76はDVDディスク、77はマイクロコンピュータ、78はサーボ手段、79はDVD誤り訂正手段、80はIEEE1394I/F、81はDVDビデオ/オーディオデコーダ、82はディジタル出力端子、83はアナログ出力端子である。

【0054】次に、本実施形態の動作を説明する。

【0055】ここではまず、動画や音声データを例えばMPEGなどの方式で圧縮し、RTRWフォーマットに変換して記録するDVD-RAMドライブの動作について説明する。DVD-RAMドライブ70への信号入力としては、ディジタル信号で入力される場合と、アナログ信号で入力される場合とがある。そのため、DVD-RAMドライブ70は、どちらの信号に対しても処理が可能ないように処理手段を備える必要がある。それぞれの入力に対する動作を、図7とともに図8、9を用いて説明する。

【0056】図8は、図7におけるIEEE1394I/F72の構成を示したものである。同図において、89はIEEE1394信号受信手段、82はDTCFで採用された方式に則って複写制御を行うDTCF手段、83はCG方式に則って複写制御を行うCG処理手段、84はM6暗号のデコード手段、85はWMを検出し、それによって制御するWM検出制御手段、86は所定の暗号化を行う暗号1エンコーダ、87はトランスポートストリームをプログラムストリームに変換するTS→PS変換手段である。

【0057】IEEE1394I/Fを介してディジタル入力受け取った信号は、IEEE1394信号受信手段89で受信され、転送データがとり出される。DTCF手段82は、データ転送を行う機器間での相互の認証と暗号を解くための鍵情報の受け渡しを行い、CG処理手段83は受信した鍵情報を更新し、新たな鍵情報を記録情報として記録する。

【0058】ここで、転送データに著作権のような権利があるものは、暗号をかけることによりデータを転送途中で読み出すことができないようにしてある。IEEE1394ではM6暗号が採用されている。権利の無いものについては、暗号化されずクリアな信号として転送される。

【0059】そのため、M6暗号がかかったデータはデコード手段84によってM6暗号をデコードして、WM検出可能なデータとし、WM検出制御手段85によりWMを検出し、検出結果にしたがって、出力を制御する。WM検出の結果、不正にコピーしたデータでなく、記録媒体への記録が許可されているデータであるならば、TS→PS変換手段87によりフォーマットの変換を行ない、その後、暗号1エンコーダ86により、所定の暗号化を行い、DVD誤り訂正符号付加手段75へ送る。ここで、暗号1はM6暗号と同じ暗号を用いても構わない。同じ暗号を用いることで、暗号の復号回路も共通化が図れるため、回路を簡略することができる。

【0060】また、暗号がかかっていないデータについても、不正にコピーされた可能性があるため、WM検出を行うようにする。ここで、WMが検出された場合には、WMにしたがって制御され、必要に応じて、暗号1

エンコーダ36により、所定の暗号化を行い、DVD誤り訂正符号付加手段75へ送る。

【0061】WM検出では、ディスクに記録するためにコピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。

【0062】なお、ここではTS→PS変換手段87はWM検出制御手段85の後段で処理する例として示したが、TS→PS変換手段87の処理の後にWM検出制御を行なうようにしても構わない。すなわち、TS→PS変換処理とWM検出制御の順番は入れ替えることが可能である。例えば、図15は図8の信号の流れの一部を入れ替えたものである。

【0063】ここで、WM検出制御手段85は、IEEE1394信号受信手段89からの転送データに対してWM検出を行うものである。このWM検出が転送されたデータからそのまま検出が可能であれば、その状態から検出を行うが、例えばWM検出がトランスポートストリームや、プログラムストリームの状態のどちらかに対応したものであれば、ストリーム変換の適切な部分でWM検出を行うようにする。また、それらのストリームの中

間レベルでWM検出が可能ならば、検出に適切なレベルの信号を用いてWM検出を行うようにする。もちろん、一旦ストリームの変換を行い、WMを検出した後に再び元のトリームに変換しても構わない。また、TS→PS変換が必要ない場合には、変換を行わずにWM検出し、出力することも可能である。

【0064】また、再生データがMPEG圧縮によるビットストリームであるのに対して、ベースバンドの状態からの検出に対応したWM検出であれば、一旦ビットストリームからベースバンドに変換してWMを検出し、その後

に元の状態に逆変換して戻すようにする。ここで、変換するレベルは、完全にベースバンドまで変換しなくても、WM検出が可能な段階まで変換を行えば良い。

【0065】このように、WM検出が可能なレベルまでデータ状態を変換するための構成とすることにより、余分な回路の増加を防止することが出来る。ここでは、MPEG圧縮と転送ストリーム変換について述べたが、WM検出するために必要があれば、WMの検出方式に併せた変換もしくは変換の一部を行い、WM検出後にもとの状態に逆変換することにより、最適にWM検出を行うことが可能となる。また、この変換はWM

の書き換えや追加が必要な場合にも適応させることが出来る。

【0067】図9は、図7におけるDVDビデオ/オーディオエンコーダ74の構成を示したものである。同図において、91はADコンバータ、92はMPEGエンコーダ、93はWM検出制御手段、94はM6暗号エンコーダ、95は暗号2エンコーダである。

【0068】映像信号や音声信号などのアナログ信号は、ADコンバータ91によりデジタル化される。ここでは図示していないが、映像信号の場合には、通常、マクロビジョン信号と呼ばれるコピー防止信号が付加されており、この信号が検出された場合には、コピーを禁止するように制御する。

【0069】次に、デジタル化されたデータはMPEGのような圧縮方式で圧縮される。

【0070】同時にWM検出制御手段93により、WMを検出し、WMが検出された場合にはWMにしたがって制御される。WMが検出されなかったり、データに権利が無いことを示すWMであった場合には、記録するデータを暗号化する必要はないので、MPEGエンコードの後、そのままDVD誤り訂正符号付加手段75へ送る。

【0071】WM検出の結果、不正にコピーしたデータでなく、記録媒体への記録が許可されているデータであるならば、M6暗号エンコーダ94または暗号2エンコーダ95により、所定の暗号化を行い、DVD誤り訂正符号付加手段75へ送る。WM検出では、ディスクに記録するためにコピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。ここで、暗号2はM6暗号またはM1暗号と同じ暗号を用いても構わない。同じ暗号を用いることで、暗号の復号回路も共通化が図れるため、回路を簡略することができる。

【0072】このように、図8、9で示したIEEE1394I/F72、および、DVDビデオ/オーディオエンコーダ74からの出力を受け取り、図7のDVD誤り訂正符号付加手段75において、誤り訂正のための符号を付加するとともに、DVDディスク76に記録できるフォーマットに変換する。マイクロコンピュータ77は、記録再生のためのシステム制御を行い、サーボ手段78をコントロールして、DVDディスクの回転やアクセスを制御する。また、図8で示したCG処理における鍵情報のやり取りも行う。

【0073】再生時も、記録時と同様デジタル出力系とアナログ出力系があり、それぞれの出力に対する動作を、図7とともに図10、11を用いて説明する。

【0074】図10は、図7におけるIEEE1394I/F70の構成を示したものである。同図において、101はCG (Contents Guard) 方式に則って複写制御を行うCG処理手段、102はDTCPで採用された方式に則って複写制御を行うDTCP手段、103はM6暗号のデコード手段、104はCSS (Contents Scram

ble System) のデコード手段、105は暗号1のデコード手段、106は暗号2のデコード手段、107はWMを検出し、それに従って制御するWM検出制御手段、108はプログラムストリームをトランスポートストリームに変換するPS→TS変換手段、109はM6暗号エンコーダ、110はIEEE1394信号受信手段である。

【0075】DVDディスクから再生されたデータは、DVD誤り訂正手段79で復調及び誤り訂正され、デジタル出力系とアナログ出力系へ送られる。

【0076】CG処理手段101は、データ中に含まれた鍵情報を更新し、新たな鍵情報を記録情報としてDTCP手段102へ送る。DTCP手段102は、データ転送を行う機器間での相互の認証と暗号を解くための鍵情報の受け渡しを行う。ここで、転送データに著作権のような権利があるものは、暗号をかけることによりデータを転送途中で取り出しても正しく読むことができないようにして転送する。

【0077】権利の無いものについては、暗号化せずクリアな信号として転送する。

【0078】誤り訂正後のデータは暗号がかかっている場合には、暗号化された方式に従ってデコードを行う。DVD-ROMディスクのデータには、CSSの暗号がかけられており、これに対応したデコーダ(デコード手段104)が必要である。記録時には、デジタル入力系とアナログ入力系で、M6暗号と暗号1、暗号2の3種の暗号があったため、これらの対応した3種のデコーダ(デコード手段103、105、106)を記したが、仮にこれらが同じ暗号を用いて記録されている場合には、それに対応してデコーダは兼用できる。各デコーダによりWM検出可能なデータまでデコードし、WM検出制御手段107によりWMを検出し、検出結果にしたがって、出力を制御する。

【0079】WM検出の結果、不正に記録されたデータでなく、データの転送が許可されているデータであるならば、プログラムストリームをトランスポートストリームに変換するPS→TS変換手段108により、ストリームを変換してから、M6暗号エンコーダ109により暗号化を行い、IEEE1394信号受信手段110へ送る。

【0080】また、暗号がかかっていないデータについても、不正にコピーされた可能性があるため、WM検出を行うようにする。ここでWMが検出された場合には、WMにしたがって制御され、PS→TS変換手段108により、ストリームを変換してから、必要に応じてM6暗号化を行い、IEEE1394信号受信手段110へ送る。

【0081】WM検出ではコピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。仮に、記録時にWMの更新が既に行われていて、再生時に

必要が無ければ更新は行わない。

【0082】なおここでも、図4で先に説明したのと同様に、PS→TS変換処理とWM検出制御の順番は入れ替えることが可能であり、図14のように信号の流れの一部を入れ替えることが可能である。

【0083】このように、WM検出するために必要があれば、WMの検出方式に併せた変換もしくは変換の一部を行い、WM検出後にもとの状態に逆変換することにより、最適にWM検出を行うことが可能となる。また、この変換はWMの書き換えや追加が必要な場合にも適応させることが出来る。

【0084】図11は、図7におけるDVDビデオ/オーディオデコーダ81の構成を示したものである。同図において、111はM6暗号のデコード手段、112はCSSのデコード手段、113は暗号1のデコード手段、114は暗号2のデコード手段、115はMPEGデコーダ、116はWM検出制御手段、117はDAコンバータである。

【0085】DVDディスクから再生されたデータは、DVD誤り訂正手段79で復調及び誤り訂正され、デジタル出力系とアナログ出力系へ送られる。

【0086】誤り訂正後のデータは暗号がかかっている場合には、暗号化された方式に従ってデコードを行う。DVD-ROMディスクのデータには、CSSの暗号がかけられており、これに対応したデコーダ(デコード手段112)が必要である。記録時には、デジタル入力系とアナログ入力系で、M6暗号と暗号1、暗号2の3種の暗号があったため、これらの対応した3種のデコーダ(デコード手段111、113、114)を記したが、仮にこれらが同じ暗号を用いて記録されている場合には、それに対応してデコーダは兼用できる。各デコーダにより復号され、MPEGデコーダ115により映像信号と音声信号にデコードされる。

【0087】ここで、WM検出制御手段116によりWMを検出し、検出結果にしたがって、出力を制御する。WM検出の結果、不正に記録されたデータでなく、データの出力が許可されているデータであるならば、DAコンバータ117を介してアナログ出力端子73から出力する。また、暗号がかかっていないデータについても、不正にコピーされた可能性があるため、WM検出を行うようにする。ここでWMが検出された場合にはWMにしたがって制御される。

【0088】WM検出ではコピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。仮に、記録時にWMの更新が既に行われていて、再生時に必要が無ければ更新は行わない。

【0089】ここでは図示していないが、映像信号の場合には、通常、マクロビジョン信号と呼ばれるコピー防止信号が付加されるため、DAコンバータ117によりデジタル化されたアナログ出力にも、同様にマクロビ

ジョン信号を付加して、コピーを禁止するように制御する。

【0090】このように、ディジタル入出力端子とアナログ入出力端子を備える記録再生装置で、データにかけられた暗号に対応して、適切な復号手段とWM検出制御手段を備えることにより、ディジタルデータ及びアナログデータのどちらに対しても適切なコピー制御を行うことが可能となる。なお、前述した2つの実施形態では、ディジタル入出力端子とアナログ入出力端子の両方を備えた機器として示したが、夫々単独での組み合わせも可能である。

【0091】ここで、図8、9、10、11の説明において、説明をわかりやすくするためWM検出制御手段を独立に示したが、記録系側においてWM検出制御手段85とWM検出制御手段93とを兼用することも可能であり、また、再生系側においてWM検出制御手段107とWM検出制御手段116とを兼用することも可能である。

【0092】図12は、DVDビデオ／オーディオデコーダの別の例を示したものであり、本例は、PCに接続されるビデオ／オーディオボードへの適用例である。

【0093】図12において、118はディジタル入力端子、119はアナログ出力端子、120はPC用ビデオ／オーディオボード、121はPC内部バスのインターフェイス、122は認証、及び鍵情報の受け渡しを行う認証手段、123はM6暗号のデコード手段、124はCSSのデコード手段、125は暗号1のデコード手段、126は暗号2のデコード手段、127はMPEGデコーダ、128はWM検出制御手段、129はDAコンバータである。

【0094】DVDドライブなどにより再生されたディジタルデータは、PCに接続されるMPEGビデオ／オーディオボードに送られ、映像信号はモニタに出力され、音声信号はスピーカから出力される。

【0095】PC内部バスのインターフェイス121は、例えばPCIのようにPC内部で、ボード間を接続するバスであったり、SCSIやATAPI、USBのように外部の機器との接続のためのデータ転送インターフェイスであったり、特に限定はしない。

【0096】データ転送を行うためには、認証手段122により接続する相手を確認し、鍵情報の受け渡しを行う。転送されるディジタルデータに、暗号がかかっている場合には、暗号化された方式に従ってデコードを行う。DVD-ROMディスクのデータには、CSSの暗号がかけられており、これに対応したデコーダ（デコード手段124）が必要である。DVDディスクに記録するには、M6暗号と暗号1、暗号2の3種の暗号が考えられるため、これらの対応した3種のデコーダ（デコード手段123、125、126）を記してある。ここでは、3種のデコーダを別別に示したが、仮にこれらが同

じ暗号方式を用いて記録されている場合には、それに対応してデコーダは兼用できる。各デコーダにより復号され、MPEGデコーダ127により映像信号と音声信号にデコードされる。

【0097】ここで、WM検出制御手段128によりWMを検出し、検出結果にしたがって、出力を制御する。WM検出の結果、不正に記録されたデータでなく、データのアナログ出力が許可されているデータであるならば、DAコンバータ129を介してアナログ出力端子119から出力する。

【0098】また、暗号がかかっていないデータについても、不正にコピーされた可能性があるため、WM検出を行うようにする。ここでWMが検出された場合には、WMにしたがって制御される。WM検出ではコピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。仮に、記録時にWMの更新が既に行われていて、再生時に必要が無ければ更新は行わない。

【0099】ここでは図示していないが、映像信号の場合には、通常、マクロビジョン信号と呼ばれるコピー防止信号が付加されるため、DAコンバータ117によりディジタル化されたアナログ出力にも、同様にマクロビジョン信号を付加して、コピーを禁止するように制御する。

【0100】図13は、IEEE1394 I/Fを備えたSTB（Set Top Box）の構成の1例を示したものである。

【0101】図13において、130はSTB、131はディジタル入力端子、132はIEEE1394信号受信手段、133はDTCPで採用された方式に則って複写制御を行うDTCP手段、134はCG方式に則って複写制御を行うCG処理手段、135はM6暗号のデコード手段、136はMPEGデコーダ、137はWMを検出し、それに従って制御するWM検出制御手段、138はDAコンバータ、139はアナログ出力端子である。

【0102】STB130は、例えば図1に示したようなDVD記録再生装置から、IEEE1394を介してディジタルデータを受け取る。IEEE1394信号受信手段132で受信された転送データは、DTCP手段133により、データ転送を行う機器間での相互の認証と暗号を解くための鍵情報の受け渡しを行い、CG処理手段134は、受信した鍵情報を更新し、新たな鍵情報を記録情報として記録する。

【0103】ここで、転送データで著作権のような権利があるデータは、暗号をかけることによりデータを転送途中で読み出すことができないようにしてあり、IEEE1394ではM6暗号が採用されている。権利の無いものについては、暗号化されずクリアな信号として転送される。

【0104】そのため、M6暗号がかかったデータはM

6 暗号をデコードして、映像や音声信号としてデコードできるようにする。MPEGデコーダ136は、復号されたデータを映像信号と音声信号にデコードする。

【0105】ここで、WM検出制御手段137によりWMを検出し、検出結果にしたがって、出力を制御する。WM検出の結果、不正に記録されたデータでなく、データの出力が許可されているデータであるならば、DAコンバータ138を介してアナログ出力端子139から出力する。また、暗号がかかっていないデータについても、不正にコピーされた可能性があるため、WM検出を行10うようにする。ここでWMが検出された場合には、WMにしたがって制御される。

【0106】WM検出ではコピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。既にWMの更新が既に行われていて、再生時に必要が無ければ更新は行わない。

【0107】ここでは図示していないが、映像信号の場合には、通常、マクロビジョン信号と呼ばれるコピー防止信号が付加されるため、DAコンバータ138により20デジタル化されたアナログ出力にも、同様にマクロビジョン信号を付加して、コピーを禁止するように制御する。

【0108】なお、図12、13では、デジタル入力20でアナログ出力を備えた装置の例を示したが、入出力の組み合わせはこれらに限定されることはなく、また、複数の入出力を備えることも可能である。

【0109】このように、デジタル入出力端子とアナログ入出力端子を備える記録再生装置で、データにかけられた暗号に対応して、適切な復号手段とWM検出制御手段を備えることにより、デジタルデータ及びアナログデータのどちらに対しても適切なコピー制御を行うことが可能となる。

【0110】

【発明の効果】以上のように本発明によれば、デジタル入出力及びアナログ入出力を備えたビットストリーム記録再生装置またはRTRW記録再生装置などにおいて、適切なWM検出制御手段と暗号のエンコード/デコードを備えることにより、著作権のあるデータが不正に記録あるいは再生されることを防止できる。

【図面の簡単な説明】

【図1】本発明の1実施形態に係る、複写制御情報を含むデータを記録再生する記録再生装置の構成を示すブロック図である。

【図2】図1のIEEE1394I/F12の構成例を示すブロック図である。

【図3】図1のDVDビデオ/オーディオエンコーダ1

4の構成例を示すブロック図である。

【図4】図1のIEEE1394I/F20の構成例を示すブロック図である。

【図5】MPEG-2システムの2種のストリームの構成の違いを示す説明図である。

【図6】図1のDVDビデオ/オーディオエンコーダ21の構成例を示すブロック図である。

【図7】本発明の他の実施形態に係る、複写制御情報を含むデータを記録再生する記録再生装置の構成を示すブロック図である。

【図8】図7のIEEE1394I/F72の構成例を示すブロック図である。

【図9】図7のDVDビデオ/オーディオエンコーダ74の構成例を示すブロック図である。

【図10】図7のIEEE1394I/F80の構成例を示す説明図である。

【図11】図7のDVDビデオ/オーディオエンコーダ81の構成例を示すブロック図である。

【図12】本発明のさらに他の実施形態に係る、再生出力系のDVDビデオ/オーディオデコーダの構成例を示すブロック図である。

【図13】本発明のさらに他の実施形態に係る、IEEE1394I/Fを備えたSTBの構成の1例を示したブロック図である。

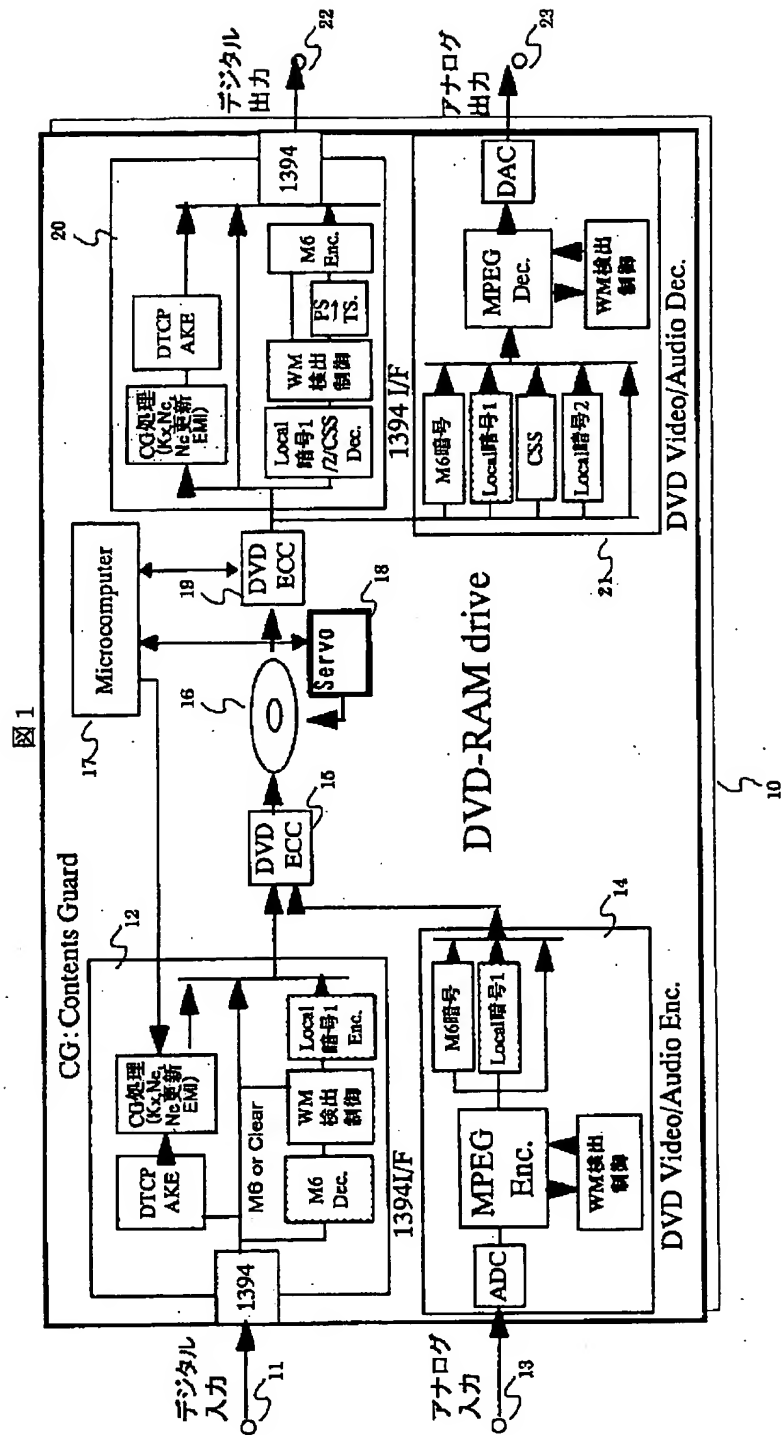
【図14】図4のIEEE1394I/F20または図10のIEEE1394I/F70の他の構成例を示すブロック図である。

【図15】図8のIEEE1394I/F72の他の構成例を示すブロック図である。

【符号の説明】

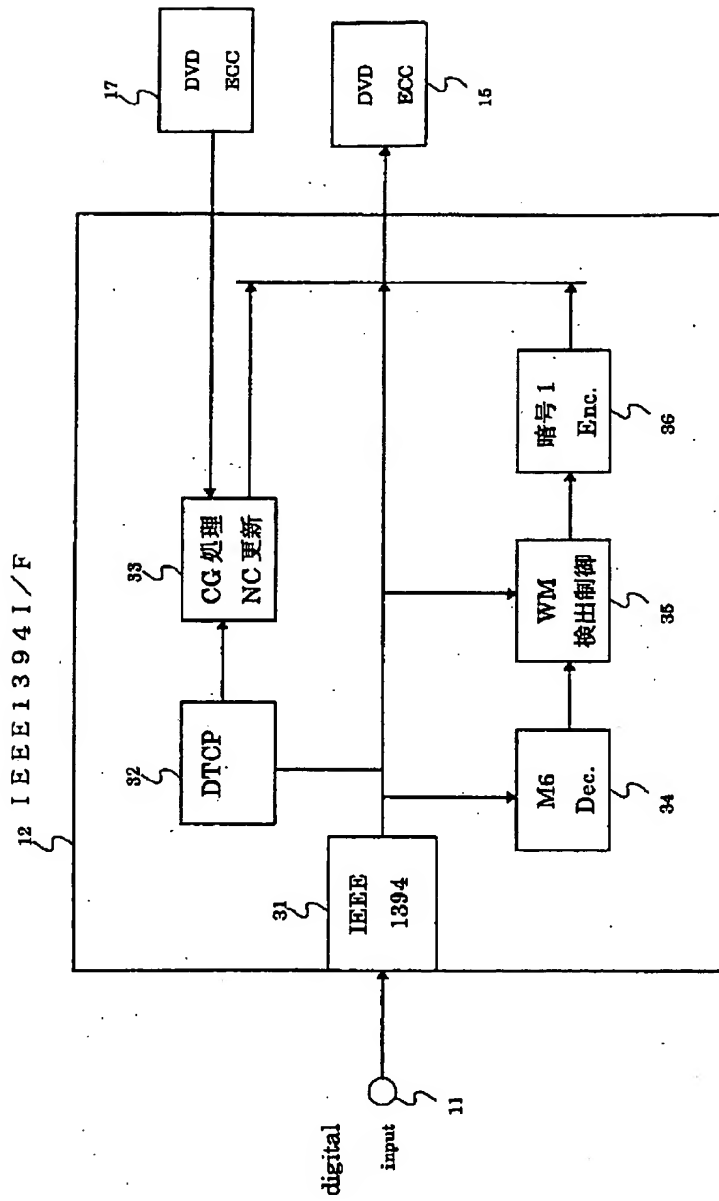
- 10 ビットストリーム記録再生可能なDVD-RAMドライブ
- 11 デジタル入力端子
- 12 IEEE1394I/F
- 13 アナログ入力端子
- 14 DVDビデオ/オーディオエンコーダ
- 15 DVD誤り訂正符号付加手段
- 16 DVDディスク
- 17 マイクロコンピュータ
- 18 サーボ手段
- 19 DVD誤り訂正手段
- 20 IEEE1394I/F
- 21 DVDビデオ/オーディオデコーダ
- 22 デジタル出力端子
- 23 アナログ出力端子

【図1】



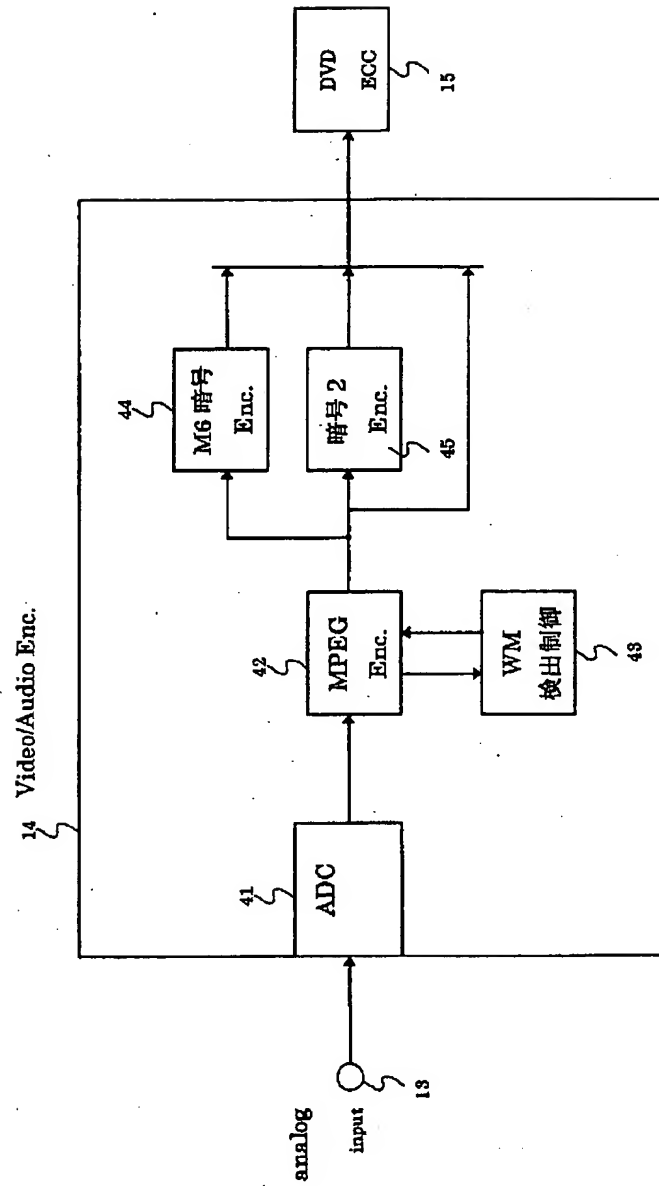
【図2】

図 2

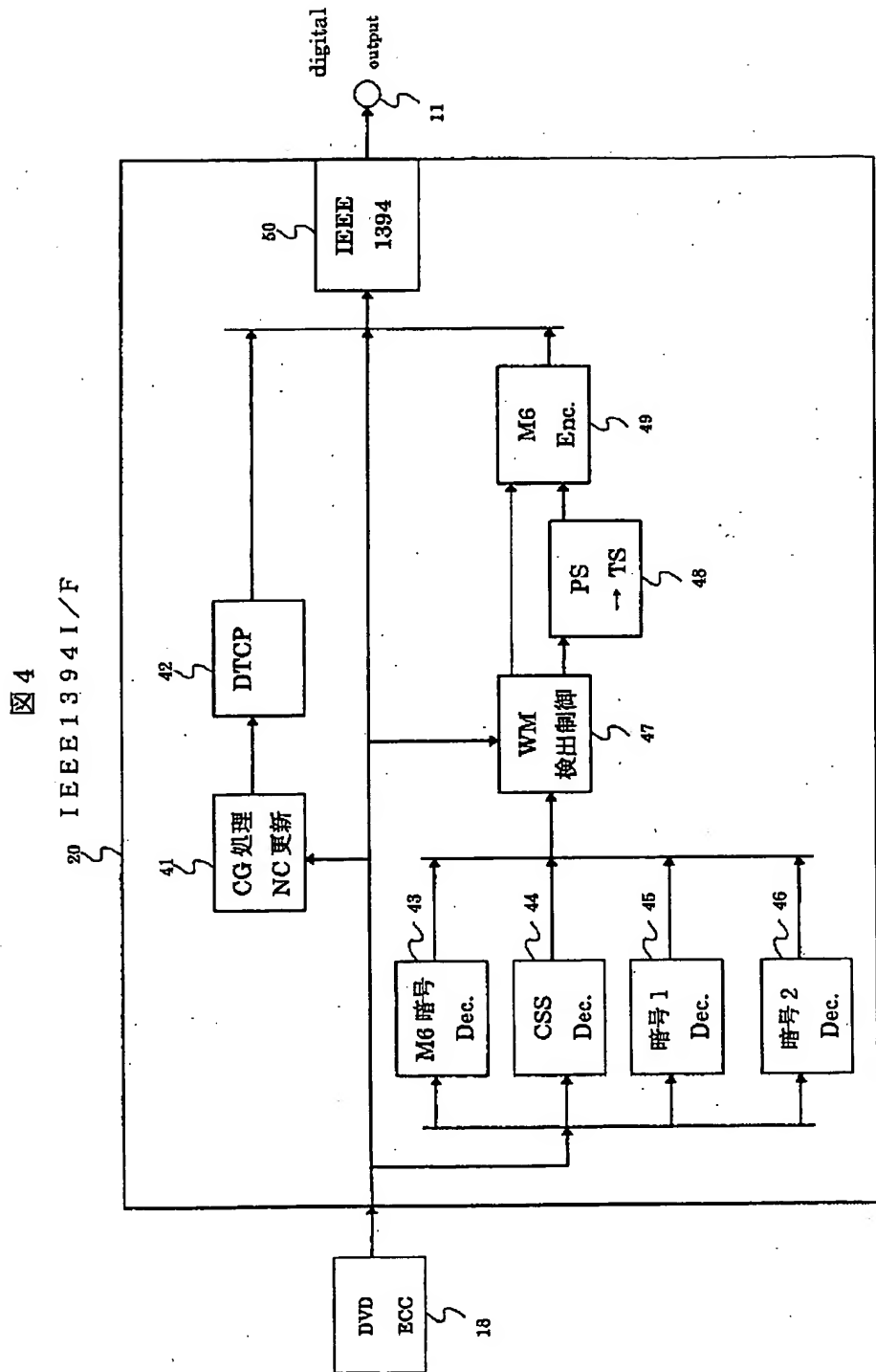


【図3】

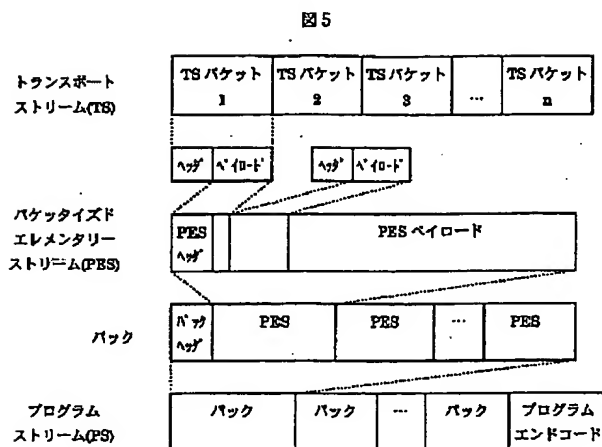
図3



【図4】

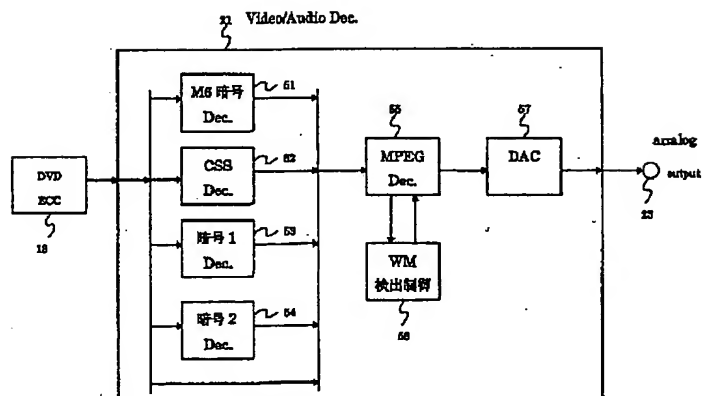


【図5】

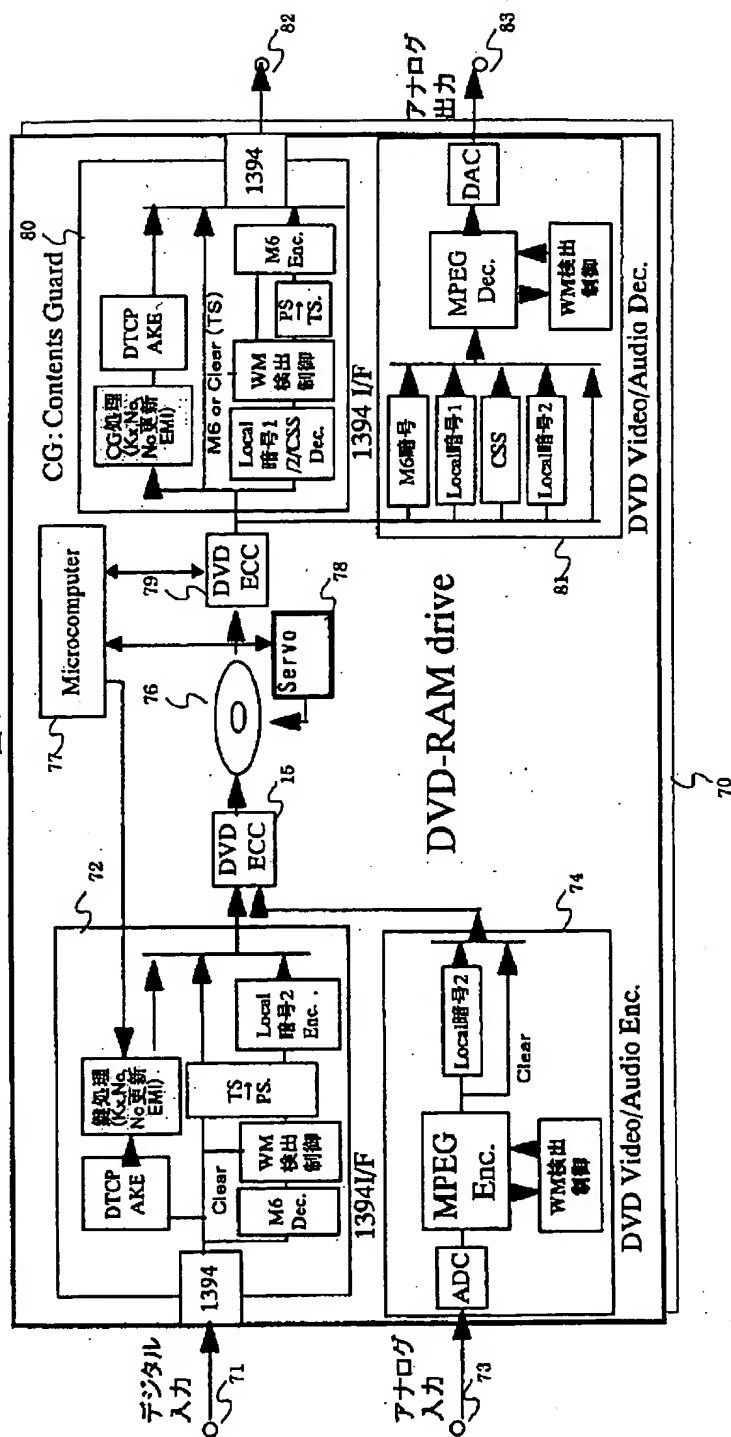


【図6】

図6

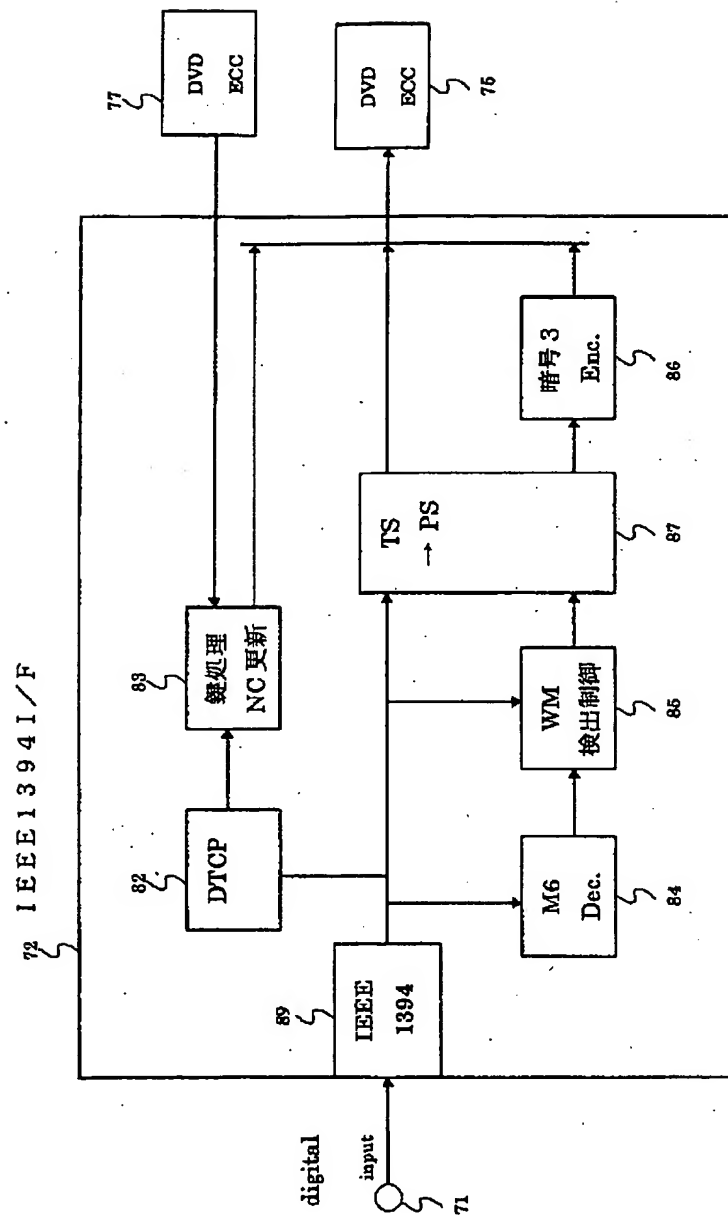


7 ☒



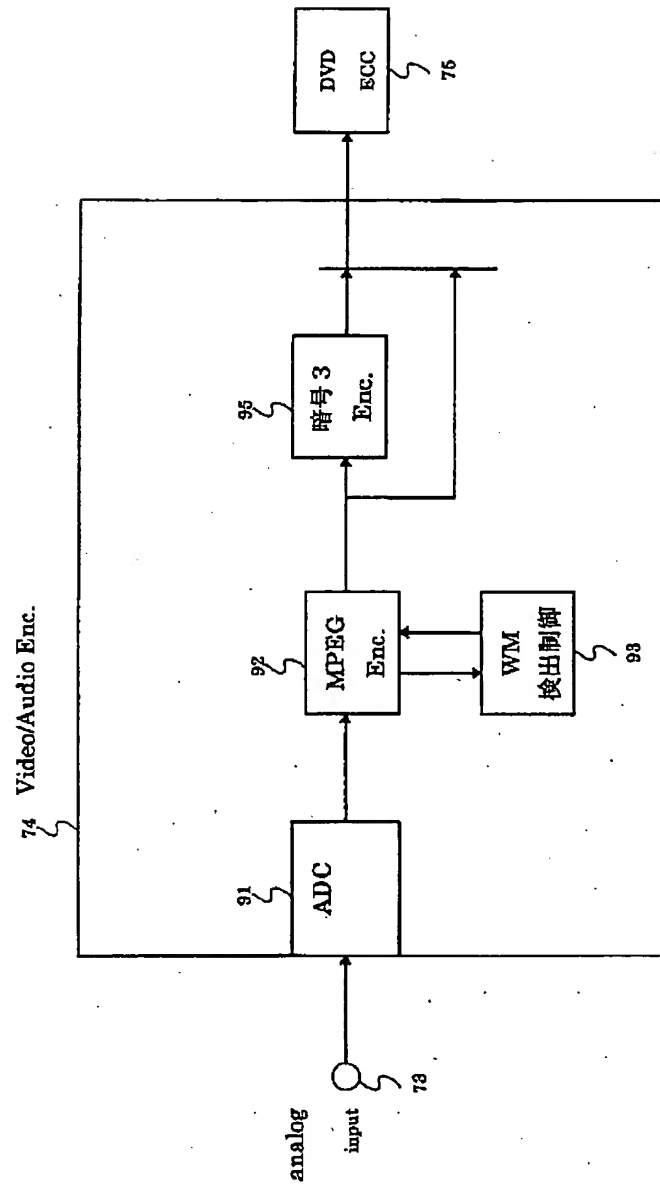
【図8】

図8

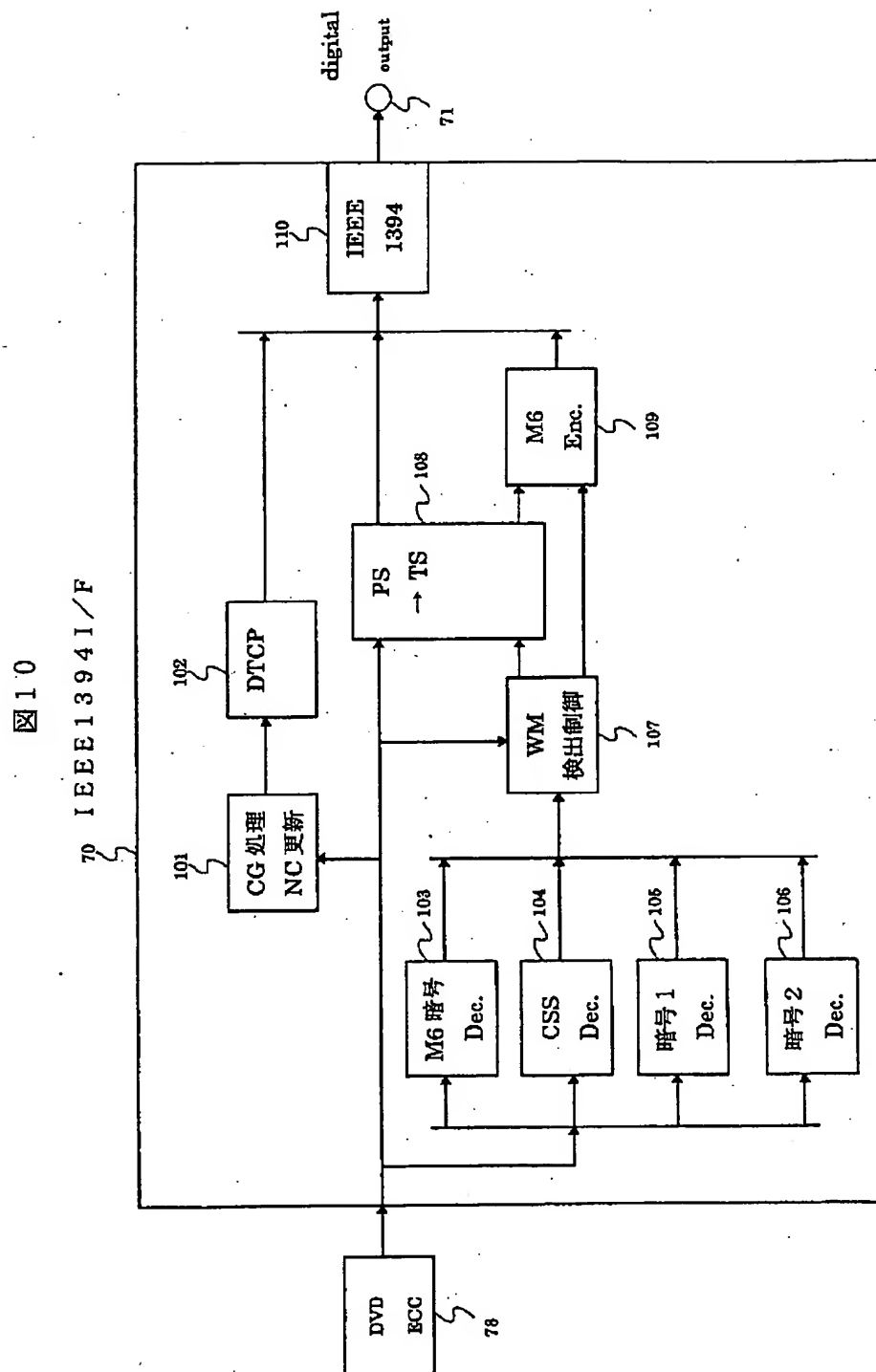


【図9】

図9

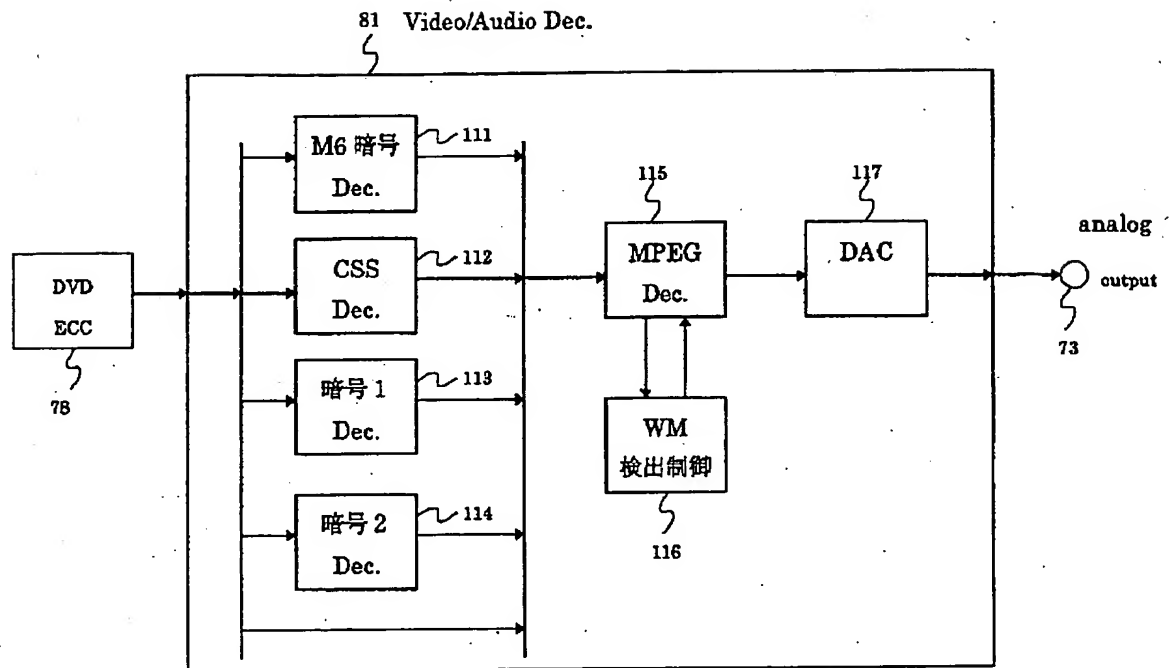


【図10】

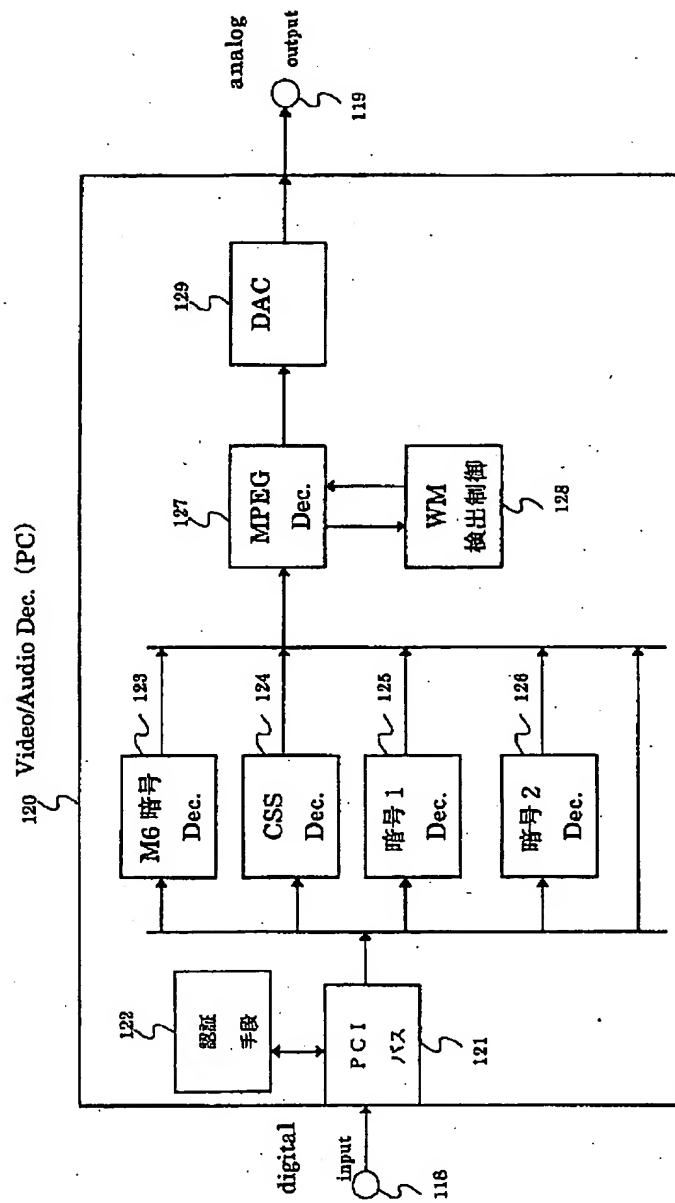


【図11】

図11

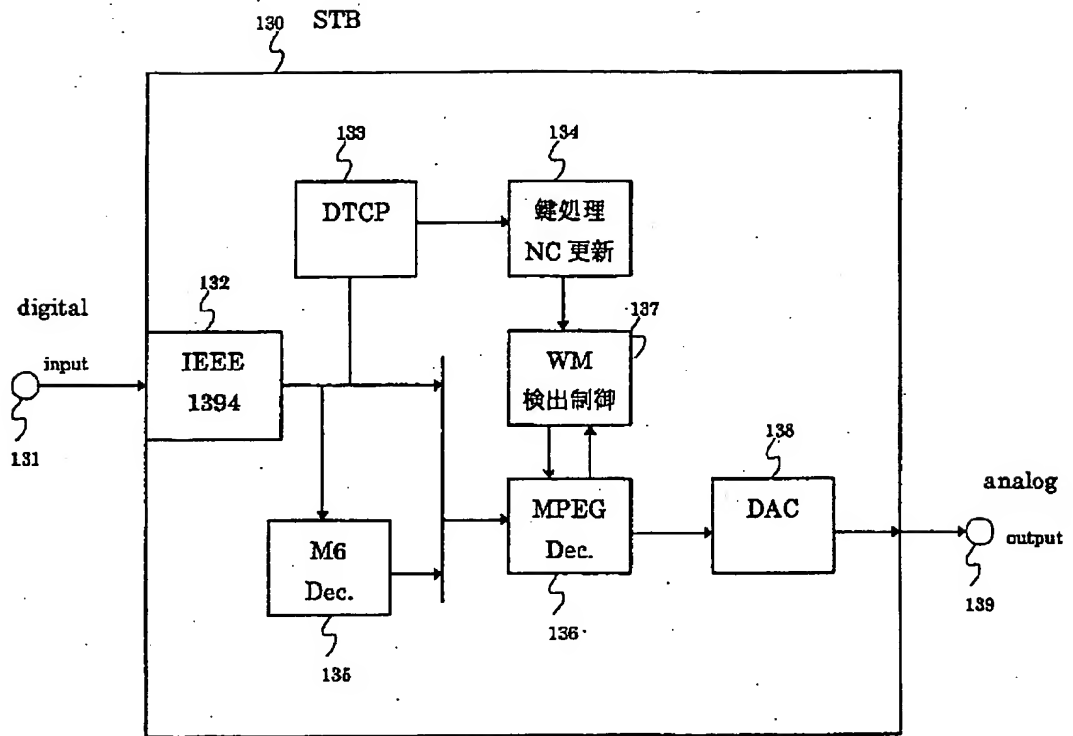


【図12】

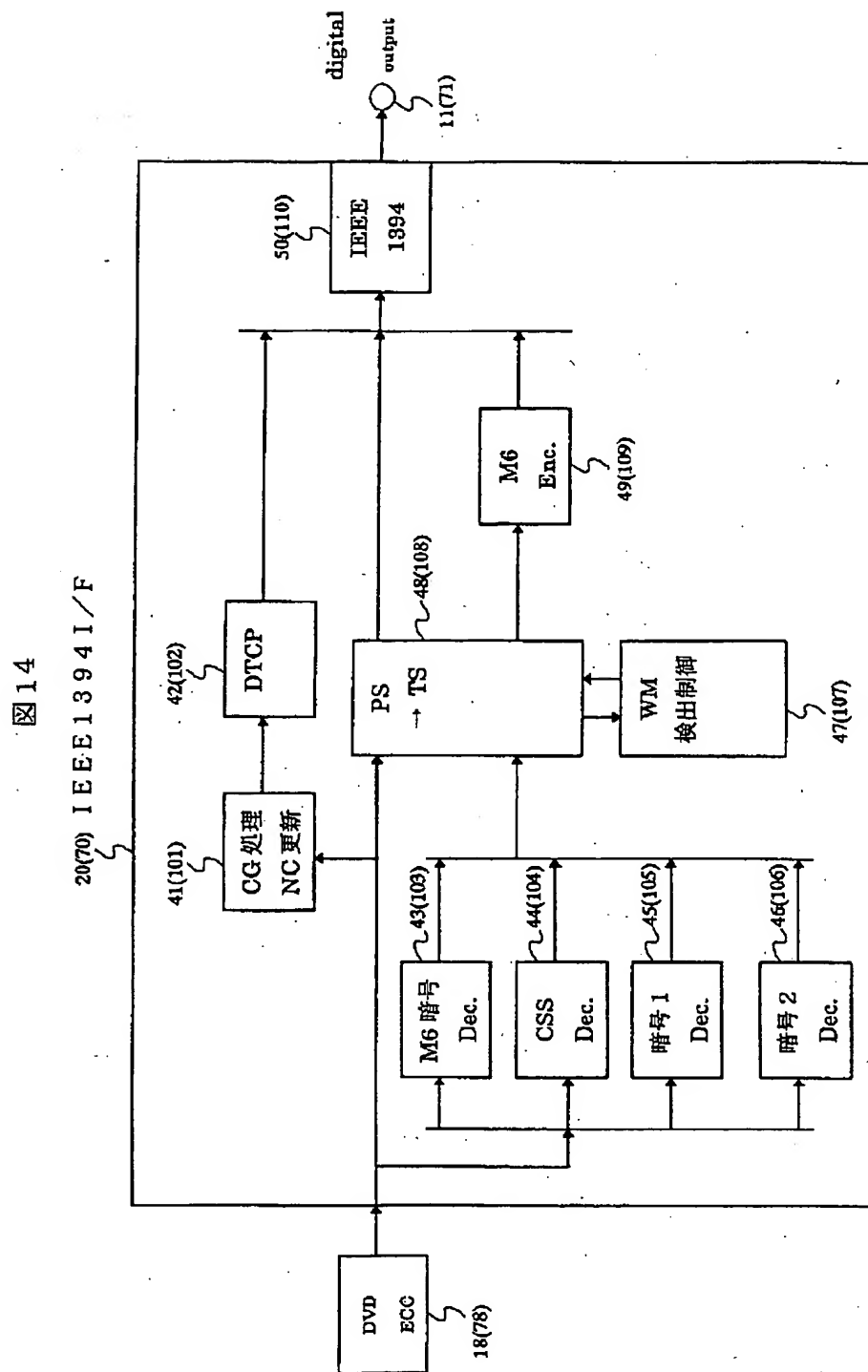


【図13】

図13



【図14】



(72)発明者 野口 敬治

神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所デジタルメディア開発本
部内

Fターム(参考) 5B017 AA06 BA07 BB09 CA09 CA15
5B057 AA11 BA04 CA12 CA16 CB12
CB16 CE08 CH11 DA08 DB02
5C053 FA25 GA10 GA11 GB05 GB38
HA33 JA16 KA04 KA25 LA11
5C076 AA14 BA06
5D044 AB01 AB05 AB07 BC06 CC04
DE50 EF01 EF05 FG14 FG18
GK07 GK17 GK20 HL02 HL08
5J104 AA14 JA31 NA02 PA14
9A001 BB02 BB03 BB04 CC02 EE02
EE03 EE05 HH15 HH27 JJ13
JJ19 JZ76 KK43 KK45 KK60
LL03